UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/762,051	06/20/2001	Heikki Einola	PM 276663	7538

909 7590 06/15/2004

PILLSBURY WINTHROP, LLP
P.O. BOX 10500
MCLEAN, VA 22102

EXAMINER	
D AGOSTA, STEPHEN M	

ART UNIT	PAPER NUMBER
2683	13

DATE MAILED: 06/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/762,051	EINOLA ET AL.	
	Examiner	Art Unit	
	Stephen M. D'Agosta	2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 May 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments filed 5-26-04 have been fully considered but they are not persuasive:

1. The abstract sent with the amendment overcomes the examiner's objection.

2. The applicant argues that the prior art cited does not teach a second cipher key for ciphering in a second network and that Raivisto teaches calculating a cipher key. The examiner disagrees since he broadly interprets Raivisto's "security method" (see abstract) as teaching any/all operations required to provide encrypted communications (ie. select and/or calculate a key, encrypt information, transmit data as well as having the far end receive, select/calculate key and decrypt information). Encrypted communications is well known in the art and inherently requires the use (eg. calculation/selection) of an encryption key. The examiner therefore interprets Raivisto as reading on the applicant's claims.

3. The applicant argues that Lintulampi does not correct deficiencies relating to selection/calculation of second cipher key. The examiner disagrees since Lintualampi teaches a dual-mode phone that, when combined with Raivisto's use of two different security methods/keys (abstract), can require multiple cipher keys if the two networks it operates on use different cipher keys – eg. one network can be more secure than the other and hence would require a second, "stronger" key, 56bit vs. 128bit DES encryption as is known in the art. Since Lintulampi teaches two different networks, one skilled would provide for a separate key for each of the two networks. The combination of Raivisto's security measures with Lintulampi's dual-mode phone would provide motivation to for use of two cipher keys in two/multiple networks.

4. The applicant argues that Luo does not correct deficiencies relating to selection/calculation of second cipher key – the examiner disagrees. Similarly to the argument from #3 above, Luo teaches secure encrypted communications via wireless means (eg. using public encryption keys which require encryption/decryption keys for

each user/network) which, when combined with Raivisto's use of two different security methods/keys (abstract), combines to read on the applicant's claims.

5. The first office action is shown below for **informational purposes** only.

6. Also included is a newly signed IDS form since the examiner missed initialing one of the references.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Ravisto U.S. Patent No. 6,081,601 in view of Lintulampi WO98-59513 and Luo US 5,909,491.

As per **claims 1, 12 and 19-20**, Raivisto teaches a method of arranging data protection in a telecommunication network including first and second mobile networks and a mobile station supporting both mobile networks comprising:

Ciphering traffic between the mobile and the first network using a fist cipher key (abstract, figures 1-9 and C4, L64-66)

But is silent on Calculating a second cipher key to be used for ciphering traffic between the mobile and the second network in the first mobile network when the mobile operates in the first network

Transmitting information necessary for calculating the second cipher key from the first mobile network to the mobile station when the mobile operates in the first mobile network

Calculating the second cipher key at the mobile station to be used for ciphering traffic between the mobile station and the second mobile network.

The examiner notes that Raivisto teaches a "mediator" (eg. SMS-C) that provides calculation of the second cipher key and transmittal of the encrypted message (with second cipher key) to the second mobile (eg. recipient). Therefore a dual-mode/multi-mode phone that has processing capability to perform cipher calculation and transceivers for multiple systems is required (and is taught below).

Lintulampi teaches a dual mode phone that can operate in both GSM and UMTS networks (eg. while roaming and then for a hand-off) [abstract]. Further to this

point is **Luo** who teaches secure communication over multiple networks whereby the phone encrypts/decrypts data (abstract, figures 1-3 and C2, L18-37, specifically L32-35). Hence, using Lintulampi and Luo would move the functionality of the SMS-C (eg. mediator) in Raivisto to the phone as is disclosed by the applicant.

With further regard to claim 20, handoffs are known in the art and are inherently taught by **Lintulampi** - dual mode phone that can operate in both GSM and UMTS networks (eg. while roaming and then for a hand-off) [abstract].

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that the mobile performs cipher calculations for multiple networks and handovers, to provide means for overcoming the single-point failure of the mediator/SMS-C which would bring the entire system down if it failed.

As per **claims 2 and 13**, Raivisto teaches claim 1 **but is silent on** further comprising:

Ciphering traffic between the mobile and the second network using the second cipher key if the mobile station is handed over from the first mobile network to the second network during an active connection.

Raivisto teaches the invention being applied to ANY wireless network (C4, L28-29) which perform inter/intra-system handovers. Hence, one skilled in the art would expect that the mobile user would be handed over from a first network to a second network and the operating parameters would change accordingly (ie. air interface and cipher) which is shown in figures 6-7 and discussed in C4, L54 to C5, L64).

Lintulampi teaches a dual-mode phone that can be handed-off between different cellular systems (ie. GSM and UMTS). One skilled knows the air interface would change as well as operating parameters such as the encryption cipher used.

It would have been obvious to one skilled in the art at the time of the invention to occurs, to provide means for using different keys on different networks for improved security.

As per **claims 3 and 14**, Raivisto teaches claim 1 **but is silent on** further comprising:

Transmitting the second cipher key from the first mobile network to the second mobile network

Transmitting the second cipher key calculated at the mobile to a ciphering mobile of the mobile station in response to a request from the first network to handover to the second network

Ciphering traffic between the mobile station and the second network using the second key after handover is complete.

Raivisto teaches use of two ciphering keys whereby the selection of keys is performed by a "mediator" instead of the mobile (abstract). One skilled in the art would provide for a dual-mode phone that can operate on two different networks as well as have cipher calculation/selection capability to off-load that function from the mediator to the phone.

Lintulampi teaches a dual mode phone that can operate in both GSM and UMTS networks (eg. while roaming and then for a hand-off) [abstract]. Further to this point is **Luo** who teaches secure communication over multiple networks whereby the phone encrypts/decrypts data (abstract, figures 1-3 and C2, L18-37, specifically L32-35). Hence, using Lintulampi and Luo would move the functionality of the SMS-C (eg. mediator) in Raivisto to the phone as is disclosed by the applicant.

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that the second key is used when handoff to a second network occurs, to provide means for improved security by changing keys when a new network is used for communications.

As per **claim 4**, Raivisto teaches claim 1 **but is silent on** further comprising:

Determining, in the first network, whether the mobile supports the second mobile network

Calculating the second cipher in the first network in response to a determination that the mobile station supports the second network

Transmitting a request for calculation of the second cipher key from first network to the mobile

Calculating the second cipher at the mobile station in response to the request for calculation of the second key.

Lintulampi teaches a dual-mode phone which can operate in GSM and UMTS modes. One skilled in the art realizes that a dual-mode phone will only register and operate in the "second system" if it is capable of communicating with it. Hence, Lintulampi inherently will check to see if the second network is compatible with the dual-mode phone's transceivers AND if so, proceed with performing cipher calculations for the second network (as taught by Raivisto).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that a second cipher is used if the phone can connect to the second network, to provide means for improved security by changing keys when a new network is used for communications.

As per **claims 5 and 15**, Raivisto teaches claim 4 **but is silent on** wherein the second cipher key is calculated in the first network when an identifier transmitted by the mobile indicates that the mobile station support the second network.

Lintulampi teaches a dual-mode phone which can operate in GSM and UMTS modes. One skilled in the art realizes that a dual-mode phone will only register and operate in the "second system" if it is capable of communicating with it. Hence, Lintulampi inherently will check to see if the second network is compatible with the dual-mode phone's transceivers ***(or identifiers)*** AND if so, proceed with performing cipher calculations for the second network (as taught by Raivisto).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that an identifier is used, to provide means for quickly determining if the phone can connect to a second network.

As per **claims 6 and 16**, Raivisto teaches claim 1 **but is silent on** further comprising:

Calculating the second cipher at a first element in the first network in response to a request from a second element of the first mobile network, the second element including identifiers transmitted by the mobile station

Transmitting the second cipher key from the first element to the second element (figures 6, 8-9 show the network containing a mediator/SMS-C which is comprised of multiple elements and provide cipher calculation).

As per **claim 7**, Raivisto teaches claim 1 **but is silent on** wherein the mobile includes a USIM application for the first network and a subscriber identification SIM application for the second mobile further comprising:

Transmitting information necessary to calculate the second cipher key received by the mobile station to the SIM application.

Luo teaches a security process by issuing a subscriber identity module(SIM) to each system user. The SIM is a plug-in chip or card that must be inserted into a mobile station that a user intends to make or receive calls through. The SIM contains a 128 bit number called the Ki that is unique for each user. The Ki is used for both authentication and deriving an encryption key. In GSM a challenge and response procedure is used to authenticate each user and generate encryption bits from Ki for the user. The challenge and response procedure may be executed at the discretion of the home system (C2, L7-17).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that a SIM with SUB-ID SIM application is used, to provide means a SIM card to off-load encryption/decryption computing from the phone's processor.

As per **claims 8-9 and 17-18**, Raivisto teaches claim 7 **but is silent on** further comprising:

Calculating the second cipher in first network in connection with an authentication response for first mobile network and first cipher key

Transmitting information necessary for calculating the first cipher key and the second cipher key, such as a random-number parameter, from first network to mobile

Transmitting information necessary for calculating the first and second cipher keys from the mobile to the subscriber identification applications for first and second networks

Calculating the second cipher key in the subscriber identification application for the second mobile network and calculating the authentication response in the subscriber identification application for the first mobile network

Acknowledging the authentication of the mobile station in the second mobile network in response to the first mobile network accepting the authentication response transmitted by the mobile

***With further regard to claims 17-18,* See claim 7 for discussion regarding USIM limitation).**

Luo teaches both an "authentication response" and use of a "random number parameter":

a. In IS-136 and IS-95 authentication and encryption, a 32-bit global challenge is generated and broadcast at predetermined intervals within systems in the service area of the mobile. When a mobile attempts system registration/call setup access in the home system, the current global challenge response is used to compute, in the mobile, an 18-bit authentication response from the mobile's SSD. An access request message, including the authentication response and a call count value for the mobile, is then sent to the home system from the mobile. Upon receiving the access request the home system will compute its own response value using the global challenge and the mobile's SSD. If the mobile is verified as authentic, by comparison of the authentication responses, the mobile's SSD and other relevant data, including the call count value, the mobile is registered (C2, L57 to C3, L4).

b. When a GSM mobile is operating in its home system, after the user has identified himself by sending in his international mobile system identity/temporary mobile system identities(IMSI/TMSI), a 128-bit random number(RAND) is generated in the system and combined with the mobile user's Ki to generate a 32-bit response (SRES). The system then transmits RAND to the mobile which, in turn, computes its own SRES value from the mobile user's Ki, and transmits this RAND back to the system. If the two SRES values match, the mobile is determined to be authentic. Encryption bits for communications between the mobile and systems are generated in both the mobile and network by algorithms using RAND and Ki to produce an encryption key "Kc". Kc is then used at both ends to provide secure communications. When a GSM mobile is roaming, the RAND, SRES and Kc values are transferred to a visited system upon registration of the user in the visited system or, upon a special request from a visited system. The Ki value is never available other then in the home system and the user's SIM (C2, L18-37).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that authentication response and random numbers are used, to provide improved security by checking for an authentication response and use of random number generator to increase difficulty of code cracking.

As per **claim 10**, Raivisto teaches claim 1 **but is silent on** wherein the second key is calculated by shortening the first cipher key in the first network and at the mobile station before a handover to the second network takes place.

Raivisto teachs first and second cipher/encryption keys (C5, L15-28). The examiner interprets the difference between the two keys as reading on the difference taught by the applicant (eg. shortening the first cipher key).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that the first key is shortened, to provide means for calculating a new second key via virtually any algorithm (ie. shorten code, lengthen code, add/subtract a number to each cipher value, etc.)

As per **claim 11**, Raivisto teaches claim 1 **but is silent on** wherein the second cipher key is calculated in response to a decision in the first network to carry out a handover to the second network.

Lintulampi teaches a dual-mode phone which can operate in GSM and UMTS modes. One skilled in the art realizes that a dual-mode phone will only register and operate in the "second system" if it is capable of communicating with it. Hence, Lintulampi inherently will check to see if the second network is compatible with the dual-mode phone's transceivers AND if so, proceed with performing cipher calculations for the second network (as taught by Raivisto).

It would have been obvious to one skilled in the art at the time of the invention to modify Raivisto, such that the second key is calculated when the phone can handoff to another network, to provide means reducing wasteful operations by first ensuring the phone can operate in a second network before calculating a new cipher.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Stephen M. D'Agosta whose telephone number is 703-306-5426. The examiner can normally be reached on M-F, 8am to 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bill Trost can be reached on 703-308-5318. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Stephen D'Agosta
6-8-04

WILLIAM TROST
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600